(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2003 (30.05.2003)

PCT

(10) International Publication Number
WO 03/044710 A1

(51) International Patent Classification[7]: G06F 17/60, G07F 7/10

(21) International Application Number: PCT/SG01/00205

(22) International Filing Date: 11 October 2001 (11.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TRUSTCOPY PTE LTD** [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119631 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WU, Jian, Kang** [CN/SG]; Blk 51, Teban Gardens #06-565, Singapore 600051 (SG). **ZHENG, Lei** [CN/SG]; Blk 3, Normanton Park #23-177, Singapore 118999 (SG).

(74) Agents: **KANG, Alban** et al.; Alban Tay Mahtani & De Silva, 39 Robinson Road, #07-01, Robinson Point, Singapore 068911 (SG).

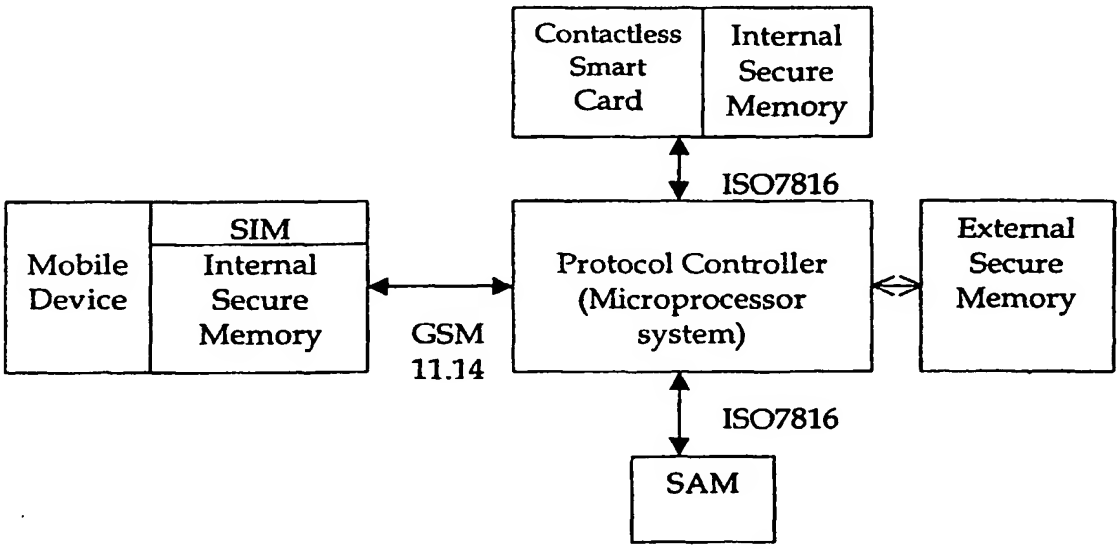
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS, METHOD AND SYSTEM FOR PAYMENT USING A MOBILE DEVICE



(57) Abstract: Apparatus for performing a payment transaction, the apparatus including a mobile device having a telecommunications means, the telecommunications means including an antenna and a subscriber identity card for communication with the mobile device; the subscriber identity card being able to obtain account information of the customer from a smart card of the customer so that an amount for the payment transaction is debited to the smart card, the mobile device being able to use the telecommunications means to communicate with a terminal to effect the payment transaction to the terminal thereby crediting the amount to the terminal; there being no requirement for physical contact between the antenna and the terminal to effect the payment transaction. Also disclosed are methods of effecting a payment transaction at a point-of-sale terminal, and at a remote terminal.

WO 03/044710 A1

Apparatus, Method and System for Payment Using a Mobile Device

Field of the Invention

The invention relates to apparatus for performing a payment or other similar transaction using a mobile device, and a method and system for performing such transactions.

Definitions

Throughout this specification reference to a smart card means a card form of a material body with a chip or module embedded in a special cavity. Examples of smart cards can be found in the white paper "Smart-Card Devices and Applications" dated January 2001 by Dustin Sorenson and found at www.dell.com/us/en/biz/topics/vectors_2001-smartcard.htm The smart card may be a contactless smart card that uses an inbuilt antenna; a smart card that has contacts and thus requires physical contact with a terminal to operate; or a hybrid smart card that has both the antenna and contacts and can operate as a contact smart card and/or as a contactless smart card.

Throughout this specification reference to a mobile device means a device for wireless communication or a device that includes one or more components for wireless communication; and includes a hand telephone, mobile telephone, cellular telephone, Personal Digital Assistant with telecommunications facilities, and laptop and notebook computers with telecommunications facilities.

Throughout this specification reference to a contactless device or smart card means such a device or smart card with no visible module that communicates by means of a radio frequency signal, and where there is no need for physical contact between the device and another device for communication between them, even though such physical contact may take place.

Background to the Invention

Payment has long been a key issue in both electronics commerce and mobile commerce. Payment applications can be classified into different categories when considered from different aspects, each of which corresponds to different requirements and different transaction procedures. Payment applications can be separated into different categories based on the location of the payment terminal. A local payment relates to the transaction process from the customer to a local payment terminal, while a remote payment is the payment between the customer and a remote payment terminal.

The present invention has as its primary objective a new apparatus or device that is useable for both local and remote payment applications as well as a new method and system to protect the security of the transaction based on that apparatus.

Consideration of the Prior Art

WO01/56313 discloses payment for a location-dependant service using mobile positioning. The invention relates to an arrangement and a method for paying for location-dependant service using a mobile phone as a positioning device. The location-dependant service may include the likes of a gas station, car wash or a train or subway station. The user of the mobile device initiates a request/order of the service or goods. The service provider offering the service or goods will determine the geographical position of the cellular device. Based on the approximate geographical position determined, the service location will provide the service or goods.

WO01/55984 discloses a flexible electronic system for conducting a commercial transaction. A computer-based system is provided in which commercial transactions can be conducted by a plurality of participating system members. Each member has a mobile device adapted to communicate with a general computerized server over an associated wireless network the server has a financial database record allocated to each member, and a plurality of merchants (each of which by definition has a financial data base record in the computerized server). The server is programmed such that financial transactions can be conducted by

remote operation of the mobile device of a participating system member, via the wireless network, to result in the debiting of a financial data base record associated with an instructing participating system member, and the crediting of a different financial data base record of another participating system member or a merchant. The system is flexible in that the server is further programmed to:

i) receive, in respect of transactions initiated otherwise than by way of the said mobile device, requests for the payment of an amount from a financial data base record of a participating system member;

ii) communicate a message seeking authorization of such payment to the mobile device associated with the relevant participating system member;

iii) receive a secure authorization signal approving of or rejecting the payment wherein such authorization signal is transmitted from the mobile device at the instance of the relevant participating system member; and

iv) thereafter effect further processing of the payment or reservation request upon receipt of such authorization signal.

WO01/55979 describes a payment device and method for secure payment. It relates to the implementation of data-secure payment services and devices. In particular, the invention relates to payment service equipment (PS) and to two methods in which PS is used. The paying with a payment card may be implemented via an information network such as the Internet in such a way that the payment is secure, and the number of the client's payment card does not need to be transmitted over the data transmission network. The client is requested to provide a separate confirmation for effecting the payment. The information to be confirmed is sent to the terminal device of the client, preferably a mobile station, by means of which the client digitally confirms the order made by signaling the confirmation. The signed confirmation, as well as the electronic identity information associated with the client, is sent back to the PS. The PS verifies the

client's identity, check the validity of the client's payment card, and transmits the payment information to the payment system.

WO01/48707 describes a smart card payment terminal. In order to solve the problem of mobile terminal operational costs, the invention provides that said payment terminals should operate in mixed mode in that it is capable of being connected both to a public mobile telephone network base station and to a private telephone network base station. The transmission mode selecting means are arranged such that preferably the private telephone network is favored since the tariff costs of such communications are less expensive.

WO01/25979 relates to a method for billing Internet transactions via a mobile radiotelephone service. By using WAP (Wireless Application Protocol), it is possible to select and, optionally, reserve goods and services (information, tickets, CD's, hotel rooms, etc) sold via the Internet. When the customer decides to purchase the goods or services, they conduct a payment transaction from the mobile radiotelephone device. The customer data required for conducting a payment transaction is centrally maintained in a database of a payment gateway.

WO01/09851 describes smart card transactions using a wireless telecommunications network. A smart card transaction allows a consumer to load value onto a smart card and to make purchases using a smart card with a special mobile telephone handset over the telecommunications network. For loading, the system includes a mobile telephone handset including a card reader; a gateway computer; a funds issuer computer; and an authentication computer. The mobile telephone handset receives a request from a user to load a value onto the smart card. The handset generates a funds request message that includes the value, and sends the funds request message to a funds issuer computer. The funds issuer computer debits an account associated with the user. Next, the handset generates a load request message with a cryptographic signature and sends the load request message to an authentication computer that authenticates the smart card. The handset receives a response message that includes a cryptographic signature and

an approval to load. Finally, the handset validates the second cryptographic signature and loads the value onto the smart card that is inserted into the smart card reader slot. For payment, the system includes a merchant server and a payment server. First, the handset sends an order request message to the merchant server computer, and in return receives a purchase instruction message. The handset processes the purchase instruction message locally, and sends a draw request message to a payment server computer. The payment server computer sends a debit message that includes a cryptographic signature and an approval to debit the smart card. Finally, the handset validates the cryptographic signature and debits the smart card.

WO00/48142 describes a payment terminal for accepting card payment. It concerns a payment terminal adapted for reading bankcards comprising a keyboard for inputting a confidential code, and at least a removable panel. It further comprises an antenna communicating with contactless cards, the panel indicating, in a first position, the zone for presenting the contactless card.

None of the prior art provides an integrated payment method that can be used for both local and remote transactions. Also none integrate mobile payment, Internet payment, and Point Of Sale ("POS") payments into a single system; and all utilize a mobile-phone-dependent channel to communicate, or are not concerned with local payment.

With the present invention there may be provided a "destroy-after-read" security feature that is not found in any of the prior art. It has the considerable advantage of not allowing unauthorized reuse of transaction data after the transaction has concluded.

Object of the Invention

The present invention has as its primary object the provision of a secure and integrated payment apparatus useable for both local and remote transactions.

A further object is to provide a method and system for the apparatus to protect the security of transactions.

Summary of the Invention

With the above and other objects in mind, the present invention provides apparatus for performing a payment transaction, the apparatus including a mobile device having a telecommunications means, the telecommunications means including an antenna and a subscriber identity card for communication with the mobile device; the subscriber identity card being able to obtain account information of the customer from a smart card of the customer so that an amount for the payment is debited to the smart card, the mobile device being able to use the telecommunications means to communicate with a terminal to effect the payment transaction to the terminal thereby crediting the amount to the terminal; there being no requirement for physical contact between the antenna and the terminal, to effect the payment transaction.

Preferably, the smart card is a contactless smart card. Alternatively, it may be a virtual smart card, all data of the smart card being maintained in a database controlled by a server. In a further alternative, it may be integrated with the subscriber identity card to form a hybrid subscriber identity card located within the mobile device; the account information and the amount being obtained from the hybrid subscriber identity card.

The hybrid subscriber identity card may have two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel; as well as a common memory for the subscriber identity card and the smart card. It may also have separate microprocessors for the smart card and the subscriber identity card.

The terminal may be a point-of-sale terminal, the communication between the mobile device and the point-of-sale terminal being by passing the antenna adjacent the point-of-sale terminal. The communication between the mobile device and the terminal is preferably radio frequency transmission, SMS, or over the Internet.

The mobile device and/or the telecommunications means may include a secure authentication module as an identity; and the mobile device preferably seeks approval of the payment transaction before crediting the amount to the terminal.

The communication between the telecommunications means and the smart card may be by passing the antenna adjacent the smart card; and the communication between the telecommunications means and the database may be by use of a telecommunications network.

IN another form the present invention provides apparatus for performing electronic payment transactions using a smart card, the apparatus including a mobile device having a telecommunication means for performing: at least one electronic payment transaction with and at a point-of-sale terminal using the smart card, and at least one further electronic payment transaction at and with a remote terminal using the smart card.

The telecommunications means may include an antenna and a subscriber identity card for communication with the mobile device; the subscriber identity card being able to obtain account information of the customer from a smart card of the customer so that an amount for the payment is debited to the smart card, the mobile device being able to use the telecommunications means to communicate with the point-of-sale terminal and the remote terminal to effect the payment transaction.

The payment transaction preferably credits the amount to the terminal; there being no requirement for physical contact between the antenna and the terminal to effect the payment transaction.

The smart card may be a contactless smart card or, alternatively, a virtual smart card, all data of the smart card being maintained in a database controlled by a server. In a further alternative, the smart card and the subscriber identity card are integrated to form a hybrid subscriber identity card located within the mobile device. In this case the hybrid subscriber identity card preferably has two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel.

The hybrid subscriber identity card may have a common memory for the subscriber identity card and the smart card; and the hybrid subscriber identity card may have separate microprocessors for the smart card and the subscriber identity card.

The communication between the mobile device and the point-of-sale terminal being by passing the antenna adjacent the point-of-sale terminal; and the communication between the mobile device and the point-of-sale terminal is radio frequency transmission, SMS, or over the Internet.

The mobile device or the telecommunications means may include a secure authentication module as an identity. Preferably, the mobile device seeks approval of the payment transaction before crediting the amount to the terminal. The communication between the telecommunications means and the smart card may be by passing the antenna adjacent the smart card; and the communication between the telecommunications means and the database may be by use of a telecommunications network.

In a further form, the present invention provides a method for effecting a payment transaction at and with a point-of-sale terminal by use of a mobile device having a telecommunications means; the method including:

(a) passing an antenna of the telecommunications means adjacent the terminal to enable the terminal to communicate with the telecommunications means to pass a message to the mobile device, the message including an amount required to be paid;

(b) using the mobile device to debit a smart card with the amount; and

(c) again passing, or maintaining, the antenna adjacent the terminal to enable the telecommunications means to send the amount to the terminal.

Preferably, the smart card is a contactless smart card and to debit the smart card the antenna of the telecommunications means is passed adjacent the smart card, there being communication between the smart card and the telecommunications means so that the amount is debited to the smart card and credited in the telecommunications means for sending to the terminal. Alternatively, the smart card is a virtual smart card, all data of the smart card being maintained in a database controlled by a server. In a further alternative, the telecommunications means includes a subscriber identity card, the smart card and the subscriber identity card being integrated to form a hybrid subscriber identity card located within the mobile device.

The hybrid smart card may have two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel. The mobile device may use the telecommunications means to communicate with the terminal to effect the payment transaction to the terminal thereby passing the amount to the terminal. The communication between the mobile device and the terminal may be radio frequency transmission, SMS, or over the Internet.

The telecommunications means may include a subscriber identity card for communication between the telecommunications means and the mobile device; and the mobile device may seek approval of the payment transaction before crediting the amount to the terminal.

The present invention also provides a method for effecting an electronic payment transaction between a first terminal and a second terminal, the method including the steps of the first terminal generating a random token and including the random token in a message; the first terminal sending the message with the random token to the second terminal; the first terminal receiving a payment credit and the random token from the second terminal, the random token being sent to the first terminal by the second terminal as a means to prevent the payment from being reused in an unauthorized manner; and the first terminal processing the payment credit and then destroying the random token.

In a final form, the present invention provides a method for effecting an electronic payment transaction between a first terminal and a second terminal, the method including the steps of the second terminal receiving a message containing a randomly generated token from the first terminal; the second terminal processing the message and obtaining a payment credit for the payment transaction; and the second terminal sending the payment credit and the random token to the first terminal in a payment message, the random token being sent to the first terminal by the second terminal as a means to prevent the payment message from being reused in an unauthorized manner, and for destruction.

In both forms the first terminal may be a supplier's terminal, and the second terminal is a customer's terminal; the customer's terminal preferably being a mobile device having a telecommunications means and the supplier's terminal a point-of-sale terminal.

The second terminal may have a telecommunications means and there may be included the extra steps of passing an antenna of the telecommunications means

adjacent the first terminal to enable the first terminal to communicate with the telecommunications means to pass the message to the second terminal, the message including an amount required to be paid; using the second terminal to debit a smart card with the amount; and again passing, or maintaining, the antenna adjacent the first terminal to enable the telecommunications means to send the amount to the first terminal.

The smart card may be a contactless smart card and to debit the smart card the antenna of the telecommunications means is passed adjacent the smart card, there being communication between the smart card and the telecommunications means so that the amount is debited to the smart card and credited in the telecommunications means for sending to the first terminal

The second terminal may use the telecommunications means to communicate with the first terminal to effect the payment transaction to the first terminal thereby passing the amount to the first terminal. The communication between the first terminal and the second terminal may be Radio Frequency transmission, SMS, or over the Internet.

The telecommunications means may include a subscriber identity card for communication between the telecommunications means and the second terminal; the smart card and the subscriber identity card being integrated to form a hybrid subscriber identity card located within the second terminal, the payment credit being obtained from the hybrid subscriber identity card. The hybrid subscriber identity card may have two interfaces, including a first interface for interaction with the second terminal through a physical connection, and a second interface for interaction with the first terminal using a radio frequency channel. It may also have a common memory for the subscriber identity card and the smart card; and separate microprocessors for the smart card and the subscriber identity card

The communication between the mobile device and the point-of-sale terminal is preferably by passing the antenna adjacent the point-of-sale terminal; and the

communication between the mobile device and the terminal may be radio frequency transmission, SMS, or over the Internet.

The message may include a bill for the amount, the bill preferably being combined with a certificate of the first terminal. The second terminal may encrypt the bill and information regarding the payment credit with an encryption key of the second terminal before sending to the first terminal. The second terminal may receive the payment credit from a remote payment gateway, the payment credit being passed directly from the payment gateway to an account for the first terminal.

As can be seen, the present invention in a preferred form provides a contactless smart card that interfaces with local payment terminal through a RF (Radio Frequency) channel and a remote terminal by use of a mobile device. It can therefore simplify the payment process, and provide an integrate interface for all transactions. Compared with other parallel approaches, a higher security level may be achieved by using a method and system over the proposed apparatus. It can protect the confidentiality, authentication, integrity, non-repudiation and authorization of the transaction in both the physical and protocol layers. Furthermore, it's compatibility with most existing payment devices may make it more acceptable than other parallel payment methods, which generally require costly equipment upgrades.

Transaction data may either be transferred between the customer's smart card and a local payment terminal by use of a smart card interface, preferably a contactless SIM card, or be transferred between the customer's smart card and a remote payment terminal through a mobile device network. The security in the transaction may be protected by a set of protocols over the apparatus. The payment method may provide a flexible and seamless solution to both local and remote payment applications.

Description of the Drawings

In order that the invention may be readily understood and put into practical effect, there shall now be described by way of non-limitative example only preferred embodiments of the present invention, the description being with reference to the accompanying illustrative drawings in which:

Figure 1 is an illustration of a payment system according to the present invention using two separate cards;

Figure 2 is an illustration corresponding to Figure 1 but where a contactless SIM card is used;

Figure 3 is a preferred implementation of Figure 1; and

Figure 4 is an example of a billing message.

Description of the Preferred Embodiment

To first refer to Figure 1, there is shown a smart card, that may be a contactless smart card, a smart card with contacts, or a hybrid smart card that uses contacts and/or a built-in antenna and is therefore contactless. The smart card stores the customer's account information. There is also a mobile device (a phone as illustrated) that includes a telecommunications means such as, for example, a SIM (Subscriber Identity Module) card or other form of interface device that communicates with the mobile device; and a transaction protocol that ensure the security and non-repudiation of the transaction. The telecommunications means may also include an antenna.

The smart card is a device that is passed near the antenna of the telecommunications means of the mobile device to carryout a transaction. Preferably, it has an electronic microchip and an antenna embedded inside the card body. These two components allow the device to communicate with an antenna/coupler unit without physical contact. It may have a secure memory that stores customer's account information.

The interface device between the smart card and the mobile phone is preferably, but not necessarily, the SIM card. The SIM card is a special smart card that communicates with the mobile device to provide the identity and other information of the subscriber. It also provides certain functions to control the mobile device. The standard of SIM card can be found in GSM 11.4, which is defined by The European Telecommunications Standards Institute (ETSI). If the mobile device uses a standard or protocol other than GSM, those standards or protocols may be applied and used with the present invention.

The transaction protocols are used to define and control the transaction procedure. They may vary according to different applications, and in different layers. For example, a transaction that involves a PDA may use Secure Socket Layer (SSL) protocol in the transfer layer, and may apply certain authentication protocols to communicate with a sales terminal.

To now refer to Figure 2, the smart card and the SIM card, are combined into one card - a hybrid SIM card with all of the functionality of the smart card and the protocol controller. The SIM card may have two sets of interfaces: one to interact with the mobile device through a physical connection, and an interface with a local payment terminal via an RF channel.

The method of the present invention, in one form, includes the following steps:

1) a SIM card is installed in the mobile device;
2) the mobile device can be used for mobile payment as if a cash card (no identification needed) and/or an ATM card (protected by a PIN, with limited daily withdrawal, as in what is done with debit cards at present);
3) the mobile device can be used for electronic payment as if an electronic checkbook (signature needed) and/or an electronic credit card (signature needed). With such an electronic payment, the mobile device works with a personal computer (PC). In such a case, it acts as a secure center for

authenticating the identity of all involved parties, protecting the integrity of transaction data, and managing the secure account information;

4) if the payment takes place at the POS, it is not necessary to send an SMS message; instead, an RF channel can be used;

5) if the payment takes place at a remote site, for example a person to person ("P2P") payment, it can be accomplished by using SMS; and

6) if the payment takes place using the Internet, for example an e-payment application, it can be accomplished by the network. In such a case, a PC may compose the bill and send it to the mobile device through an RF channel; the consumer can confirm the bill in the mobile device and send it back to the PC; the PC can capture the signature (if necessary); and the payment is send to the retailer using the Internet. In this instance, the PC is acting as if a local point-of-sale payment terminal.

Figure 3 shows an implementation of the embodiment of Figure 1.

A contactless smart card is preferably, but not necessarily, a microprocessor card. It has an internal embedded antenna to communicate with an antenna/coupler unit without physical contact. On the other hand, it can add, delete and manipulate information in its secure memory according to external instructions. For details, please refer to ISO/IEC 7816 for standards of IC cards and microprocessor card standards, and ISO 14443 for proximity (contactless) smart card standards.

A SIM card is a smart card for GSM systems and holds the subscriber's ID number, security information and memory for a personal directory of numbers thus allowing the subscriber to call from any GSM device. The SIM card is preferably a SIM Toolkit (STK) Card, which supports data management application for SIM cards. Please refer to ETSI GSM 11.14 for standards of SIM cards.

Transaction information on the two cards is preferably synchronized to provide an integrated account management. There are many different methods and devices to

exchange data between two smart cards. For example, an external microprocessor system may be applied to allow transparent communication between the SIM card and the smart card. It preferably supports Secure Authentication Module (SAM) in the microprocessor system so that the system can be used as a POS device. The SIM card may also share a common secure memory with the smart card to facilitate synchronization of transaction data.

When an external microprocessor system is applied, the service program that controls the microprocessor system preferably resides in a secure memory. It is also preferred for the service program to be encrypted in the memory, and only decrypted when executed. The decryption program may reside in the internal secure memory of the microprocessor, which is not accessible by external programs.

The communication between the mobile device and the mobile network may be protected by secure protocols for integrity and confidentiality during the transaction process. An example of such a protocol is WTLS (Wireless Transaction Layer Security) protocol, which is a component of an as-yet-to-be-implemented MeT (Mobile Electronic Transaction) initiative.

An example of communication procedure from the smart card to the SIM card by means of the microprocessor system may be:

1) the smart card sends a request to the microprocessor system for displaying a message on the mobile device;
2) the microprocessor system interprets the request, and sends instruction to the SIM card;
3) the SIM card interfaces with the mobile device and displays a message on the mobile device;
4) the customer responds to the message;
5) the response is captured and sent to the SIM card by the mobile device;
6) the microprocessor queries the SIM card if the response is ready, and reads the response from the SIM card when it is ready;

7) the microprocessor writes the response to the smart card; and
8) the smart card or the mobile device interacts with the external payment terminal according to the response.

As shown in Figure 2, the SIM card and the smart card in the first preferred embodiment can be combined into one card, namely, a hybrid SIM card. In such a case, the SIM card and the smart card may share a common secure memory, but use separate microprocessors.

The hybrid SIM card may interact with the mobile device with a standard SIM card interface as defined in ETSI GSM 11.14. If the mobile device is not in accordance with the GSM standard, other standards or protocols may be used. The remote transaction data may be sent to, or sent from the hybrid SIM card as a short message, an email, or a voice message by the mobile device. The hybrid SIM card interacts with a local payment terminal with a standard contactless smart card interface as defined in ISO 14443. Local transaction data may be sent to, or sent from the hybrid SIM card through a Radio Frequency (RF) channel. The hybrid SIM card also interacts with the user by displaying a message on the screen of the mobile device, and by reading the user's input from the mobile device. It is preferable that the hybrid SIM card includes a SAM (Secure Authenticity Module) or WIM (Wireless Identity Module) to provide non-repudiation for user identity.

Transaction and security protocols assume that the consumer has installed the apparatus with Public Key Infrastructure ("PKI") functionality and a public/private key pair. However, a secret key or other symmetrical encryption method can also be used if the service provider is a trusted party.

A general framework of transaction protocols may be:

1) the customer receives a bill from a payment terminal, and saves it to the mobile device;
2) the customer selects a payment method;

3) the mobile device reads the account information of the customer from the smart card or the hybrid SIM card;
4) the mobile device generates a message that includes payment information and/or bill information and/or account information;
5) a message for the customer is displayed on the mobile device, and the mobile device captures the customer's response;
6) after the customer has approved or authorized the payment, a digital signature is generated to the payment message, according to a security key assigned to the customer's account;
7) the mobile device sends the signed payment message to the payment terminal to accomplish the transaction; and
8) the payment terminal may send a receipt to the apparatus if needed or requested.

The bill may include information of the payee, transaction data, the amount of the payment required, and other related information. The related information may include a description of the goods or services, the place of transaction, and so forth. The bill may also be encoded to a short message, if necessary or requested; and may be encrypted to prevent a third party from obtaining transaction details.

The payment terminal may be a device located at the POS, a mobile payment gateway, or a server computer. It may communicate with other related parties such as, for example, one or more banks if necessary.

The customer's account information may be stored in the smart card or the hybrid SIM card by an issuing bank, a mobile service provider, or any other authorized parties. Preferably, the account information is stored in a secure memory or protected by a security algorithm to prevent a third party from accessing, tampering with, or falsifying the account information. It may include the customer's name, issuing bank's name, account number, expiring date, and so forth. It may also include the account balance when handling the immediate transfer of money.

The apparatus may then generate a payment message, which includes one or more selected from an account information, billing information, transaction audit trail, and timestamp for the transaction. It may be encoded and encrypted to form a secure short message.

A digital signature may be generated to protect the integrity and authenticity of the payment message to guarantee the non-repudiation for the duration of the transaction process.

The keys for creating the digital signature may be pre-stored in the apparatus. It may be dynamically changed for each transaction. PKI may be used for encryption and decryption.

The smart card may be a virtual smart card with all of the data normally in the memory of the smart card being held in a database controlled by a server. The customer can access the server through a gateway using their mobile device.

The embodiment may vary between different applications. In the following sections detailed description of protocols in several application scenarios are given.

1. Cash card payment in mobile payment applications

1) Paying at POS with a hybrid SIM card in the customer's mobile device:
   a) the retailer prepares a bill with the POS device. The bill includes the amount of money, time stamp, a random generated token, and other related information;
   b) the POS device signs the bill such that the bill is combined with a certificate of the POS device;
   c) the consumer moves their mobile device to be near the POS device to receive the bill over an RF channel;

d) the mobile device displays the bill, verifies that the bill comes from a certified POS device;

e) the consumer confirms the bill by pressing a key such as, for example, "OK" or "Yes";

f) the mobile device encrypts the bill and the payment information with the consumer's encryption key;

g) the mobile device sends payment authorization to the POS device through the RF channel;

h) the mobile device deducts the related amount of money from the secure memory of its hybrid SIM card; and

i) the POS device verifies the signature with integrated bill information and the random generated token, increases the amount of money in its secure memory, and destroys the token.

2) As Above But Remote Paying Process:

(a) the retailer prepares a bill with the POS/Mobile/PC device. The bill includes the amount of money, time stamp, a random generated token, and other related information;

(b) the retailer signs the bill such that the bill is combined with a certificate of the retailer;

(c) the retailer sends the signed bill to the consumer's mobile device by SMS;

(d) the consumer's mobile device displays the bill, verifies that the bill comes from a certified retailer;

(e) the consumer confirms the bill by pressing a relevant key such as, for example, "OK" or "Yes";

(f) the mobile device encrypts the bill and the payment information with the consumer's encryption key;

(g) the mobile device sends the payment information to the retailer by use of SMS;

(h) the mobile device deducts the relevant amount of money from the secure memory of its hybrid SIM card;

(i) the retailer verifies the signature with the integrated bill information, increases the amount of money in its secure memory, and destroys the token; and

(j) the retailer sends a confirmation message to the consumer's handset as a receipt.

3) "P2P" money transferring Process:

a) the service provider presets a token for each SIM card;

b) the sender signs a payment information message with their encryption key and sends it as an SMS to the receiver;

c) the sender's mobile device deducts the relevant amount of money from the secure memory of its hybrid SIM card;

d) the SMS is first passed through the service provider's SMS gateway;

e) the service provider decrypts the payment SMS by using the sender's public key;

f) the service provider generates a new token, adds the preset token and the new token to the payment SMS;

g) the service provider signs the payment SMS, sends the new SMS to the receiver;

h) the receiver's mobile device receives the SMS, verifies it by the service provider's public key, verifies the token;

i) the receiver's mobile device increases the amount of money in its secure memory;

j) the receiver's mobile device destroys the preset token, replaces it with the new token that comes with the payment SMS; and

k) the receiver may send a conformation SMS to the sender as a receipt.

4) Internet Paying Process:

This is similar to the paying process at the POS, except that the POS device is replaced by a PC, and a remote server prepares and forwards the bill through Internet.

5) Top-up Process:

This is similar to the P2P transfer, except that the sender is now an authorized device such as, for example, an ATM kiosk or the mobile device.

2. ATM card payment in mobile payment applications (protected by PIN)

1) Paying Process at POS:

a) the retailer prepares a bill with the POS device. The bill includes the amount of money, time stamp, and other related information;

b) the POS device signs the bill so that the bill is combined with a certificate of POS device;

c) the consumer passes their mobile devices near the POS device to receive the bill over an RF channel;

d) the mobile device displays the bill, verifies that the bill came from a certified POS device;

e) the consumer confirms the bill by entering their PIN number, and then pressing "OK", "Yes" or other relevant key;

f) the mobile device encrypts the bill and the payment information with the consumer's encryption key;

g) the mobile device sends the payment to the POS device through the RF channel;

h) the POS device passes the payment information to a remote payment gateway such as, for example, their bank's payment gateway;

i) the payment gateway verifies the signature with the integrated bill information, transfers the corresponding money from the consumers account to the retailer's account;

j) the payment gateway sends a conformation signal to the POS device; and

k) after receiving the conformation signal, the POS device then sends or prints a receipt for the consumer.

2) Remote Paying Process:

a) the retailer prepares a bill with the POS/Mobile/PC device. The bill includes the amount of money, time stamp, and other related information;

b) the retailer signs the bill so that the bill is combined with a certificate of the retailer;

c) the retailer sends the bill to the consumer's mobile device using SMS;

d) the mobile device displays the bill, verifies that the bill came from a certified retailer;

e) the consumer confirms the bill by entering their PIN number and then pressing "OK", "Yes" or other relevant key;

f) the mobile device encrypts the bill and the payment information with the consumer's encryption key;

g) the mobile device sends the payment to the retailer using SMS;

h) the SMS is first passed through the service provider's SMS gateway;

i) the service provider's SMS gateway passes the payment information to a remote payment gateway, such as for example, their bank's payment gateway;

j) the payment gateway verifies the signature with the integrated bill information, and transfers the corresponding money from the consumer's account to the retailer's account;

k) the payment gateway sends a conformation signal to the retailer; and

l) after receiving the conformation signal, the retailer may send a receipt to the consumer.

3) P2P money transfer Process:

a) the sender signs a payment information message with their encryption key and sends it as an SMS to the receiver;

b) the SMS is first passed through the service provider's SMS gateway;

c) the service provider's SMS gateway passes the payment information to a remote payment gateway, such as for example, their bank's payment gateway;

d) the payment gateway verifies the signature with the integrated bill information, and transfers the corresponding money from the sender's account to the receiver's account;

e) the payment gateway sends a conformation signal to the receiver; and

f) after receiving the conformation signal, the receiver may send a receipt to the sender.

4) Internet Paying Process:

This is similar to the paying process at the POS, except that the POS device is now replaced by a PC, and the bill is prepared by a remote server and sent over the Internet.

5) Account Transfer Process:

This is similar to the P2P money transfer, except that the sender is now an authorized device, such as for example, an ATM kiosk or the mobile device.

3. Electronic checkbook in electronic payment applications

This is somewhat different to the applications described above in that the issuing of an electronic checkbook requires a valid signature of the payer. There are several ways to generate a valid signature to a specific document. An example is given in our international patent application number PCT/SG01/00150 filed 16 July 2001 entitled "Electronic signing of document", the contents of which are hereby incorporated by reference.

A destroy-after-use strategy is applied to ensure that only one copy of a valid electronic check will exist at any time. The "destroy" action of the randomly generated key is performed by a secure hardware device, which is preferably tamper-proof and difficult to reverse engineer.

The process may be:

1) issuing the checkbook:

a) the consumer sends a request to the issuing bank using SMS or other relevant method;

b) the issuing bank generates a number of random tokens, encrypts them using the consumer's encryption key, and sends them to the consumer using SMS; and

c) the consumer's mobile device receives the tokens and stores them in its secure memory.

2) sending a check:

a) the consumer receives a bill over the Internet;

b) the bill is sent to the consumer's mobile device using an RF channel;

c) using a PC, the signature of the consumer is captured from a tablet and a valid hand signature for the bill is generated;

d) the captured signature is also sent to the mobile device;

e) the mobile device then integrates bill information, a preset token from the random tokens, and the captured signature into a document, encrypts the document using its private key, and sends it to the PC;

f) the mobile device destroys the used token; and

g) the consumer sends the e-check to the receiver through their PC.

3) Validating a check:

a) the receiver sends the check to the bank;

b) the bank verifies the identity of both the sender and the receiver, the authenticity of the token, the integrity of the content, and the authenticity of the signature, then transfers money to the value of the e-check from the sender's account to the receiver's account;

c) the bank then destroys the token; and

d) a confirmation may be sent to the sender and/or the receiver as a receipt.

4. Electronic credit card applications

This is somewhat similar to the electronic checkbook, except that a fixed credit card number replaces the random generated token.

The present invention therefore provides a new payment solution for both electronic commerce and mobile commerce. It provides an integrated solution for electronic payment, mobile payment and Internet payment; and is based on the widely accepted SMS service. Existing payment solutions mainly use WAP applications, which are difficult to use. Furthermore, the present invention may be compatible with all current GSM mobile devices. All a customer needs to do is to install a new SIM card, thus avoid costly upgrading of their mobile devices. It is also compatible with most existing transaction systems. Retailers may continue to use their related payment terminal and networks. Finally, it may combine with public key encryption to offer higher security and non-repudiation; and to manage the use of transaction data, therefore effectively blocking any third party from reusing or tampering with the data.

Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technical field that many variations or modifications in details may be made without departing from the present invention.

The present invention extends to all features disclosed both individually and in all possible combinations and permutations.

The Claims:

1. Apparatus for performing a payment transaction, the apparatus including a mobile device having a telecommunications means, the telecommunications means including an antenna and a subscriber identity card for communication with the mobile device; the subscriber identity card being able to obtain account information of the customer from a smart card of the customer so that an amount for the payment is debited to the smart card, the mobile device being able to use the telecommunications means to communicate with a terminal to effect the payment transaction to the terminal thereby crediting the amount to the terminal; there being no requirement for physical contact between the antenna and the terminal, to effect the payment transaction.

2. Apparatus as claimed in claim 1, wherein the smart card is a contactless smart card.

3. Apparatus as claimed in claim 1, wherein the smart card is a virtual smart card, all data of the smart card being maintained in a database controlled by a server.

4. Apparatus as claimed in claim 1, wherein the smart card and the subscriber identity card are integrated to form a hybrid subscriber identity card located within the mobile device; the account information and the amount being obtained from the hybrid subscriber identity card.

5. Apparatus as claimed in claim 4, wherein the hybrid subscriber identity card has two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel.

6. Apparatus as claimed in claim 4 or claim 5, wherein the hybrid subscriber identity card has a common memory for the subscriber identity card and the smart card.

7. Apparatus as claimed in any one of claims 4 to 6, wherein the hybrid subscriber identity card has separate microprocessors for the smart card and the subscriber identity card.

8. Apparatus as claimed in any one of claims 1 to 7, wherein the terminal is a point-of-sale terminal, the communication between the mobile device and the point-of-sale terminal being by passing the antenna adjacent the point-of-sale terminal.

9. Apparatus as claimed in any one of claims 1 to 8, wherein the communication between the mobile device and the terminal is selected from the group consisting of: radio frequency transmission, SMS, and the Internet.

10. Apparatus as claimed in any one of claims 1 to 9, wherein the mobile device includes a secure authentication module as an identity.

11. Apparatus as claimed in any one of claims 1 to 9, wherein the telecommunications means includes a secure authentication module as an identity.

12. Apparatus as claimed in any one of claims 1 to 11, wherein the mobile device seeks approval of the payment transaction before crediting the amount to the terminal.

13. Apparatus as claimed in any one of claim 2 or any one of claims 8 to 12 when appended to claim 2, wherein the communication between the telecommunications means and the smart card is by passing the antenna adjacent the smart card.

14. Apparatus as claimed in claim 3 or any one of claims 8 to 12 when appended to claim 3, wherein the communication between the telecommunications means and the database is by use of a telecommunications network.

15. Apparatus for performing electronic payment transactions using a smart card, the apparatus including a mobile device having a telecommunication means for performing: at least one electronic payment transaction with and at a point-of-sale terminal using the smart card, and at least one further electronic payment transaction at and with a remote terminal using the smart card.

16. Apparatus as claimed in claim 15, wherein the telecommunications means includes an antenna and a subscriber identity card for communication with the mobile device; the subscriber identity card being able to obtain account information of the customer from a smart card of the customer so that an amount for the payment is debited to the smart card, the mobile device being able to use the telecommunications means to communicate with the point-of-sale terminal and the remote terminal to effect the payment transaction.

17. Apparatus as claimed in claim 16, wherein the payment transaction credits the amount to the terminal; there being no requirement for physical contact between the antenna and the terminal to effect the payment transaction.

18. Apparatus as claimed in any one of claims 15 to 17, wherein the smart card is a contactless smart card.

19. Apparatus as claimed in any one of claims 15 to 17, wherein the smart card is a virtual smart card, all data of the smart card being maintained in a database controlled by a server.

20. Apparatus as claimed in claim 16 or claim 17, wherein the smart card and the subscriber identity card are integrated to form a hybrid subscriber identity card located within the mobile device.

21. Apparatus as claimed in claim 20, wherein the hybrid subscriber identity card has two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel.

22. Apparatus as claimed in claim 20 or claim 21, wherein the hybrid subscriber identity card has a common memory for the subscriber identity card and the smart card.

23. Apparatus as claimed in any one of claims 20 to 22, wherein the hybrid subscriber identity card has separate microprocessors for the smart card and the subscriber identity card.

24. Apparatus as claimed in any one of claims 15 to 23, wherein the communication between the mobile device and the point-of-sale terminal being by passing the antenna adjacent the point-of-sale terminal.

25. Apparatus as claimed in any one of claims 15 to 24, wherein the communication between the mobile device and the point-of-sale terminal is selected from the group consisting of: radio frequency transmission, SMS, and the Internet.

26. Apparatus as claimed in any one of claims 15 to 25, wherein the mobile device includes a secure authentication module as an identity.

27. Apparatus as claimed in any one of claims 15 to 25, wherein the telecommunications means includes a secure authentication module as an identity.

28. Apparatus as claimed in any one of claims 15 to 27, wherein the mobile device seeks approval of the payment transaction before crediting the amount to the terminal.

29. Apparatus as claimed in claim 18 or any one of claims 24 to 28 when appended to claim 18, wherein the communication between the telecommunications means and the smart card is by passing the antenna adjacent the smart card.

30. Apparatus as claimed in claim 19 or any one of claims 24 to 28 when appended to claim 19, wherein the communication between the telecommunications means and the database is by use of a telecommunications network.

31. A method for effecting a payment transaction at and with a point-of-sale terminal by use of a mobile device having a telecommunications means; the method including:

(d) passing an antenna of the telecommunications means adjacent the terminal to enable the terminal to communicate with the telecommunications means to pass a message to the mobile device, the message including an amount required to be paid;

(e) using the mobile device to debit a smart card with the amount; and

(f) again passing, or maintaining, the antenna adjacent the terminal to enable the telecommunications means to send the amount to the terminal.

32. A method as claimed in claim 31, wherein the smart card is a contactless smart card and to debit the smart card the antenna of the telecommunications means is passed adjacent the smart card, there being communication between the smart card and the telecommunications means so that the amount is debited to the smart card and credited in the telecommunications means for sending to the terminal.

33. A method as claimed in claim 31, wherein the smart card is a virtual smart card, all data of the smart card being maintained in a database controlled by a server.

34. A method as claimed in claim 31, wherein the telecommunications means includes a subscriber identity card, the smart card and the subscriber identity card being integrated to form a hybrid subscriber identity card located within the mobile device.

35. A method as claimed in claim 34, wherein the hybrid smart card has two interfaces, including a first interface for interaction with the mobile device through a physical connection, and a second interface for interaction with a point-of-sale terminal using a radio frequency channel.

36. A method as claimed in claim 32 or claim 33, wherein the mobile device uses the telecommunications means to communicate with the terminal to effect the payment transaction to the terminal thereby passing the amount to the terminal.

37. A method as claimed in any one of claims 31 to 37, wherein the communication between the mobile device and the terminal is selected from the group consisting of: radio frequency transmission, SMS, and the Internet.

38. A method as claimed in any one of claims 31 to 33, wherein the telecommunications means includes a subscriber identity card for communication between the telecommunications means and the mobile device.

39. A method as claimed in any one of claims 31 to 38, wherein the mobile device seeks approval of the payment transaction before crediting the amount to the terminal.

40. A method for effecting an electronic payment transaction between a first terminal and a second terminal, the method including the steps of:

(a) the first terminal generating a random token and including the random token in a message;

(b) the first terminal sending the message with the random token to the second terminal;

(c) the first terminal receiving a payment credit and the random token from the second terminal, the random token being sent to the first terminal by the second terminal as a means to prevent the payment from being reused in an unauthorized manner; and

(d) the first terminal processing the payment credit and then destroying the random token.

41. A method for effecting an electronic payment transaction between a first terminal and a second terminal, the method including the steps of:

(a) the second terminal receiving a message containing a randomly generated token from the first terminal;

(b) the second terminal processing the message and obtaining a payment credit for the payment transaction; and

(c) the second terminal sending the payment credit and the random token to the first terminal in a payment message, the random token being sent to the first terminal by the second terminal as a means to prevent the payment message from being reused in an unauthorized manner, and for destruction.

42. A method as claimed in claim 40 or claim 41, wherein the first terminal is a supplier's terminal, and the second terminal is a customer's terminal.

43. A method as claimed in claim 42, wherein the customer's terminal is a mobile device having a telecommunications means.

44. A method as claimed in claim 42 or claim 43, wherein the supplier's terminal is a point-of-sale terminal.

45. A method as claimed in any one of claims 40 to 42, wherein the second terminal has a telecommunications means; the method further including the steps of:

(a) passing an antenna of the telecommunications means adjacent the first terminal to enable the first terminal to communicate with the telecommunications means to pass the message to the second terminal, the message including an amount required to be paid;

(b) using the second terminal to debit a smart card with the amount; and

(c) again passing, or maintaining, the antenna adjacent the first terminal to enable the telecommunications means to send the amount to the first terminal.

46. A method as claimed in claim 45, wherein the smart card is a contactless smart card and to debit the smart card the antenna of the telecommunications means is passed adjacent the smart card, there being communication between the smart card and the telecommunications means so that the amount is debited to the smart card and credited in the telecommunications means for sending to the first terminal.

47. A method as claimed in claim 46, wherein the second terminal uses the telecommunications means to communicate with the first terminal to effect the payment transaction to the first terminal thereby passing the amount to the first terminal.

48. A method as claimed in any one of claims 40 to 47, wherein the communication between the first terminal and the second terminal is selected from the group consisting of: Radio Frequency transmission, SMS, and the Internet.

49. A method as claimed in any one of claims 40 to 48, wherein the telecommunications means includes a subscriber identity card for communication between the telecommunications means and the second terminal.

50. A method as claimed in claim 49, wherein the smart card and the subscriber identity card are integrated to form a hybrid subscriber identity card located within the second terminal, the payment credit being obtained from the hybrid subscriber identity card.

51. A method as claimed in claim 50, wherein the hybrid subscriber identity card has two interfaces, including a first interface for interaction with the second terminal through a physical connection, and a second interface for interaction with the first terminal using a radio frequency channel.

52. A method as claimed in claim 50 or claim 51, wherein the hybrid subscriber identity card has a common memory for the subscriber identity card and the smart card.

53. A method as claimed in any one of claims 50 to 52, wherein the hybrid subscriber identity card has separate microprocessors for the smart card and the subscriber identity card.

54. A method as claimed in claim 44, wherein the communication between the mobile device and the point-of-sale terminal is by passing the antenna adjacent the point-of-sale terminal.

55. A method as claimed in claim 54, wherein the communication between the mobile device and the terminal is selected from the group consisting of: radio frequency transmission, SMS, and the Internet.

56. A method as claimed in any one of claims 40 to 55, wherein the message includes a bill for the amount.

57. A method as claimed in claim 56, wherein the bill is combined with a certificate of the first terminal.

58. A method as claimed in claim 56 or claim 57, wherein the second terminal encrypts the bill and information regarding the payment credit with an encryption key of the second terminal before sending to the first terminal.

59. A method as claimed in claim 43, wherein the second terminal receives the payment credit from a remote payment gateway.

60. A method as claimed in claim 59, wherein the payment credit is passed directly from the payment gateway to an account for the first terminal.

61. Apparatus as claimed in any one of claims 1 to 30, when used to perform the method of any one of claims 31 to 60.

62. A method as claimed in any one of claims 31 to 60, when performed using the apparatus of any one of claims 1 to 30.

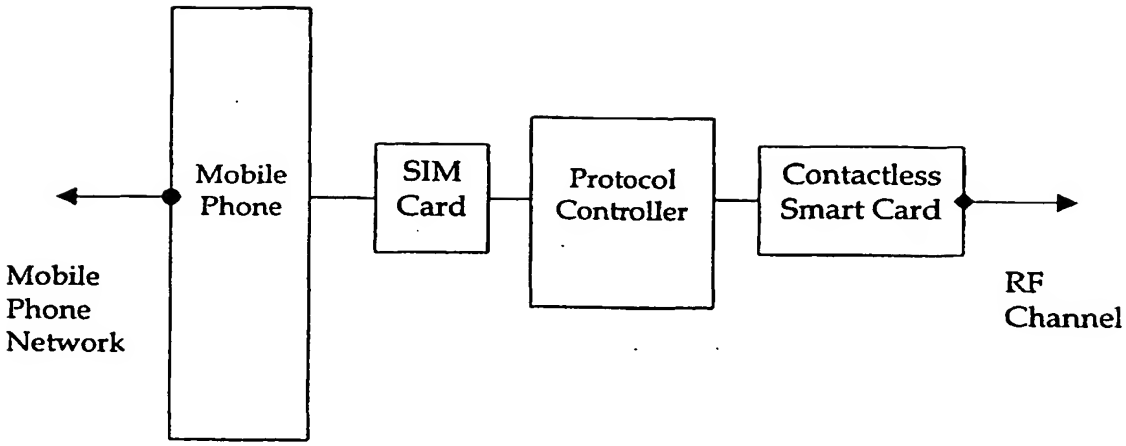

Mobile Phone
SIM Card
Protocol Controller
Contactless Smart Card
Mobile Phone Network
RF Channel

Figure 1

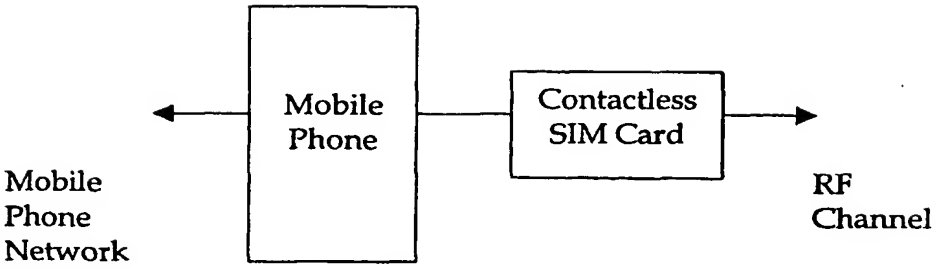

Mobile Phone
Contactless SIM Card
Mobile Phone Network
RF Channel

Figure 2

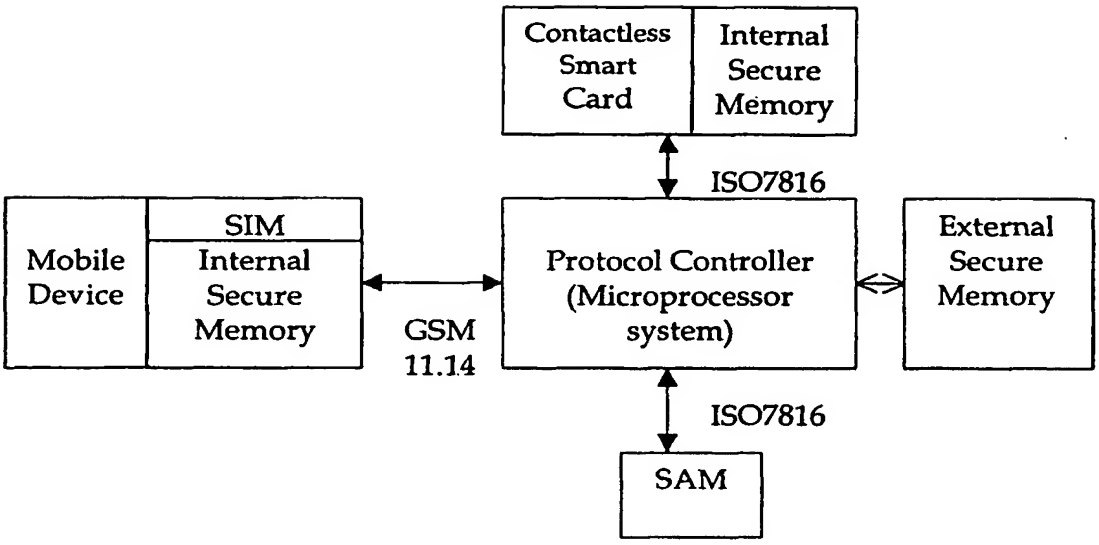

Contactless Smart Card
Internal Secure Memory
ISO7816
Mobile Device
SIM
Internal Secure Memory
GSM 11.14
Protocol Controller (Microprocessor system)
External Secure Memory
ISO7816
SAM

Figure 3

Payee	Billing Date
Total Payment Amount	Tax Information
Description of Goods	
Randomly Generated Token	Other information

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG01/00205

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/60, G07F 7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B.

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT (smart, card, SIM, payment)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/55979 (Sonera Smarttrust OY) 2 August 2001 Abstract, figures, page 23 line 30 to page 25 line 27)	1,2
X	WO 01/41036 (Dacom Cyberpass) 7 June 2001 Abstract, page 7 line 24 to page 8 line 29	1,3
X	WO 01/09851 (Visa International Service Association) 8 February 2001 Whole document	1,2,9

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 November 2001

Date of mailing of the international search report 26 NOV 2001

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. (02) 6285 3929

Authorized officer

DALE E. SIVER
Telephone No : (02) 6283 2196

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG01/00205

C (Continuation). **DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/56313 (Telefonaktiebolaget LM Ericsson) 2 August 2001 Abstract, figures	1
A	WO 01/13314 (Mantzivis) 22 February 2001 Example 2, page 9,10	1
A	WO 00/48142 (Ascom Monetal S.A.) 17 August 2000 Abstract, figures, claims	1

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG01/00205

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	2001/55979	FI	2000/0135				
WO	2001/41036	AU	2000/51146	CN	1322326		
WO	2001/09851	AU	2000/63702				
WO	2001/56313	NO	2000/56313				
WO	2001/13314	AU	2000/73911				
WO	2000/48142	AU	2000/25544	EP	1072023	FR	2789786
							END OF ANNEX